SHCreateProcessAsUserW

Use fully qualified executable filename. Do not depend on the shell's heuristics to locate the file.

Sean Barnum, Cigital, Inc. [vita[1]]

2007-04-16

Part "Original Cigital Coding Rule in XML"

Mime-type: text/xml, size: 4888 bytes

Attack Category	• Path spoofing or confusion problem
Vulnerability Category	• Indeterminate File/Path • Process management
Software Context	• Shell Functions • Process Management
Location	• shlobj.h
Description	When calling SHCreateProcessAsUserW(), care must be exercised to ensure an unauthorized executable cannot end up getting run. SHCreateProcessAsUserW() creates a new user-mode process and its primary thread to run a specified executable file. If the file to be executed is not fully specified, heuristics are used to try to find the file. Do not depend on the shell's heuristics to locate the file, as this can create vulnerabilities to attacks. Make sure you provide an unambiguous definition of the application that is to be executed. The executable filename should be fully qualified, including the file extension. If any elements of the command line string contain white space, wrap them in double quotes. Otherwise, the parser might interpret an element containing one or more spaces as multiple separate elements.
APIs	**Function Name** / **Comments** SHCreateProcessAsUserW / Not supported under XP
Method of Attack	An attacker could inject a Trojan horse executable into the system by placing a "tainted" executable in a location in the search path that is found before the intended executable.
Exception Criteria	
Solutions	**Solution Applicability** / **Solution Description** / **Solution Efficacy**

1. http://buildsecurityin.us-cert.gov/bsi/about_us/authors/35-BSI.html (Barnum, Sean)

	Whenever invoking SHCreateProcessAsUserW()	The pszFile member of the SHCREATEPROCESSINFOW parameter block should be the fully qualified path to the executable file. The pszParameters member of SHCREATEPROCESSINFOW should be the command line with each element wrapped in double quotes.	Effective, assuming SHCREATEPROCESSINFOW executable is not tainted.

Signature Details	BOOL SHCreateProcessAsUserW(PSHCREATEPROCESSINFOW pscpi);

Examples of Incorrect Code	`PSHCREATEPROCESSINFOW pscpi;`
	`pscpi.pszFile = L"My Program"; // File specification is not specific enough to be safe`
	`[...]`
	`if (! SHCreateProcessAsUserW(pscpi)) { /* handle error */ }`

Examples of Corrected Code	`PSHCREATEPROCESSINFOW pscpi;`
	`pscpi.pszFile = L"\"C:\\MyDirectory\\My Program.exe\""; // File is fully specified and properly quoted`
	`[...]`
	`if (! SHCreateProcessAsUserW(pscpi)) { /* handle error */ }`

Source Reference	• http://msdn.microsoft.com/library/default.asp?url=/library/en-us/shellcc/platform/Shell/programmersguide/sec_shell.asp[2]
Recommended Resources	• MSDN reference for SHCreateProcessAsUserW[3] • MSDN reference for CreateProcessAsUser[4]
Discriminant Set	**Operating System**: • Windows **Languages**: • C • C++

Cigital, Inc. Copyright

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

1. mailto:copyright@cigital.com